PKI Enforcement Communications

Communications Outline

1. PKI Transition – What is changing and what's the impact
2. Overall timeline of activities for PKI Transition
3. What this means for DOD Users
4. What this means for Non-DOD Users
5. Customer Support

1. PKI Transition – What is changing and what's the Impact?

DISA will change the authentication options for DISA Direct and will remove the use of passwords, in accordance with DOD Instruction 8520.02 - Public Key Infrastructure (PKI) and Public Key Enabling (PKE) – reference: http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf

Once fully implemented, all applications that rely on DISA Direct authentication (ex. DDOE, Storefront, TIBI) will be affected and they will no longer accept the use of passwords for new or existing users.

All DISA Direct users (DOD and non-DOD) will have to use DOD approved PKI solutions as the only supported method for authentication and access into DISA Direct and supported applications.

2. Overall Timeline of Activities for PKI Transition

- **Now** - all DOD users can associate individual (single) accounts to their CAC
- **12/15/2014 to 1/9/2015** - all non-DOD users with access to a DOD approved or interoperable PKI solutions can support the DISA testing effort
- **12/30/2014** - all DOD users with multiple accounts can associate them to their CAC
- **12/31/2014** - all DOD users must use CAC to access their accounts
- **2/2/2015 to 2/6/2015** - DISA allows non-DOD users with DOD approved or interoperable PKI solutions to test associating their certificates to their account
- **2/14/2015** - non-DOD users with DOD approved/interoperable PKI certificates are not allowed to user passwords for authentication
- **3/31/2015** - non-DOD users without access to a DOD approved/interoperable solution must find an alternative means to utilize the DISA Direct enabled capabilities

3. What this means for a DOD User

All DOD users have access to a DOD issued Common Access Card (CAC) which provides a PKI solution for identity verification. As such, all DOD users must associate their CAC to their existing DISA Direct accounts as soon as possible to prevent any denial in access to your existing DISA Direct account or supported applications.

For DOD Users with Single Accounts in DISA Direct

Follow the steps below to associate your CAC to your account

- Login to DISA Direct by using your existing User ID and Password
- Click on '***CAC Registration***' or go to the following link: https://www.disadirect.disa.mil/products/user/asp/secure/register_cac.asp
- Select '***Register Certificate***' on the displayed screen
- Note that you should receive a confirmation if the association to your CAC was successful

For additional instructions or resources:

- PKI/CAC First Time User Guide
- PKI/CAC FAQs

For DOD Users with Multiple Accounts in DISA Direct

For any DOD user that has multiple DISA Direct accounts (ex. multiple User IDs) follow the below steps to associate each of your User IDs to your CAC

- After associating your primary user id to your CAC, clear your cache and log out and log back into the browser
- Login to DISA Direct using the User ID and Password for next user you want to register
- Click on '***CAC Registration***' or go to the following link: https://www.disadirect.disa.mil/products/user/asp/secure/register_cac.asp
- Select '***Register Certificate***' on the displayed screen
- Repeat above steps for each user account you have

4. What this means for Non-DOD Users

Non-DOD users represent US federal agencies, local or state governments, commercial companies, and foreign affiliates or coalition partners. Most non-DOD users have access to a corporate provided PKI solution that may be DOD approved and interoperable. DISA will work to support all non-DOD users with DOD approved or interoperable PKI certificates; however DISA will require awareness of the specific type of PKI solution that is in use by a non-DOD user to ensure that it can perform adequate testing.

Verify that you have a DOD approved or interoperable PKI solution

- Visit the following site to view a list of DOD approved or interoperable PKI certificates: http://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx
- Contact your corporate IT support team to determine which PKI solution is used by your company or agency and compare that to the listing in the list above

Steps to Prepare for using a DOD approved or Interoperable PKI certificate

- If you have a PKI solution that is on the DOD approved or interoperable list, please notify DISA by performing a simple test as described below:
  1. Insert your smart card (that holds your PKI certificate) into the card reader on your computer that is internet accessible
  2. Click on the following link which will allow DISA to capture your PKI certificate profile https://www.disadirect.disa.mil/getCertInfo.asp
  3. You will get a confirmation page that displays the information provided by your certificate
  4. DISA will conduct a User Acceptance Test between 2/2/2015 and 2/6/2015 for non-DOD users that want to associate their DOD approved and interoperable PKI certificates with their existing accounts

What to do if you do not have access to a DOD approved or interoperable PKI certificate?

- If your IT support team notifies you that you do not have a corporate PKI solution, or if you do have a corporate PKI solution that is not on the DOD approved or interoperable list – then explore the options outlined below

Option	Eligibility	Requirements	Cost
Obtain a DOD issued Common Access Card (CAC)	Non-DoD Federal employees without PIV; Foreign military, foreign government or foreign government contractors	1) Obtain a DOD sponsor 2) Submit Request 3) Go To CAC office and Pic up CAC 4) Background Investigation 5) Biometrics (fingerprints, facial image) Reference: • DoD Manual 1000.13, Volume 1	Variable
Obtain an External Certificate Authority (ECA) PKI Certificate	Federal and state employees and contractors; Foreign government employees	1) Obtain a Government sponsor 2) Visit the following site to identify an ECA approved vendor http://iase.disa.mil/pki/eca/Pages/index.aspx 3) Apply with an ECA approved vendor a. Operational Research Consultants b. Symantec c. IdenTrust Reference: • http://iase.disa.mil/pki/eca/Pages/index.aspx • http://www.symantec.com/page.jsp?id=eca-certificates • http://www.identrust.com/certificates/eca/index.html • http://eca.orc.com/	Variable based on selected vendor pricing
Obtain a Personal Identity Verification	Federal employees and contractors	1) Background Investigation 2) Biometrics (fingerprints, facial image) Reference:	Variable

(PIV) PKI Certificate		• http://csrc.nist.gov/groups/SNS/piv/standards.html	

PKI Support for non-DOD Users

Beginning February 2015, DISA plans to support non-DOD users with access to a DOD approved or interoperable solution.

DISA will publish additional information on how non-DOD users can utilize PKI access into DISA Direct

5. Customer Support

Please contact the DISN Global Support Center (DGSC) for all questions on DISA Direct or locked accounts by phone or email:

- DSN: (312) 850-4790
- CML: (800) 554-3476 or (614) 692-4790
- DISA.DGSC@mail.mil
- disa.columbus.ns.mbx.dgsc@mail.smil.mil

Please note that the DGSC is only able to provide support for technical issues related to use of a valid DOD issued, approved or interoperable PKI certificate that is being used to access DISA Direct.

Please contact your local IT support staff, DOD liaison or third party vendor for all matters related to obtaining and maintaining a DOD issued, approved or interoperable PKI certificate.